# Long live the king—content, that is! With cyber security culture protection

In September, the country was hit once again with a colossal data breach. This time, one of the country's "kings" of Personally Identifiable Information (PII) was hit by a data breach impacting 143 million people. If it could happen at Equifax, it can happen anywhere. Will this be the straw that breaks the camel's hack—I mean, back?

On October 2, we began observing the 14th annual National Cyber Security Awareness Month (NCSAM). A little late for Equifax. We can only hope that this will be the year we can feel secure again in our digital world—or at the very least not experience another earth-shattering cyber security event. Into our second decade of cyber security awareness, we should be seeing less cyberattacks—not more.

NCSAM is a collaborative effort launched in 2004 by the Department of Homeland Security and the National Cyber Security Alliance—with the goal of bringing cyber security awareness to consumers, businesses, educational institutions and government organizations—to make us aware of the rampant cyber threats and how to protect our privacy and confidential information from scams like spear phishing.

**Okay—now that we're aware, what do we do next?**

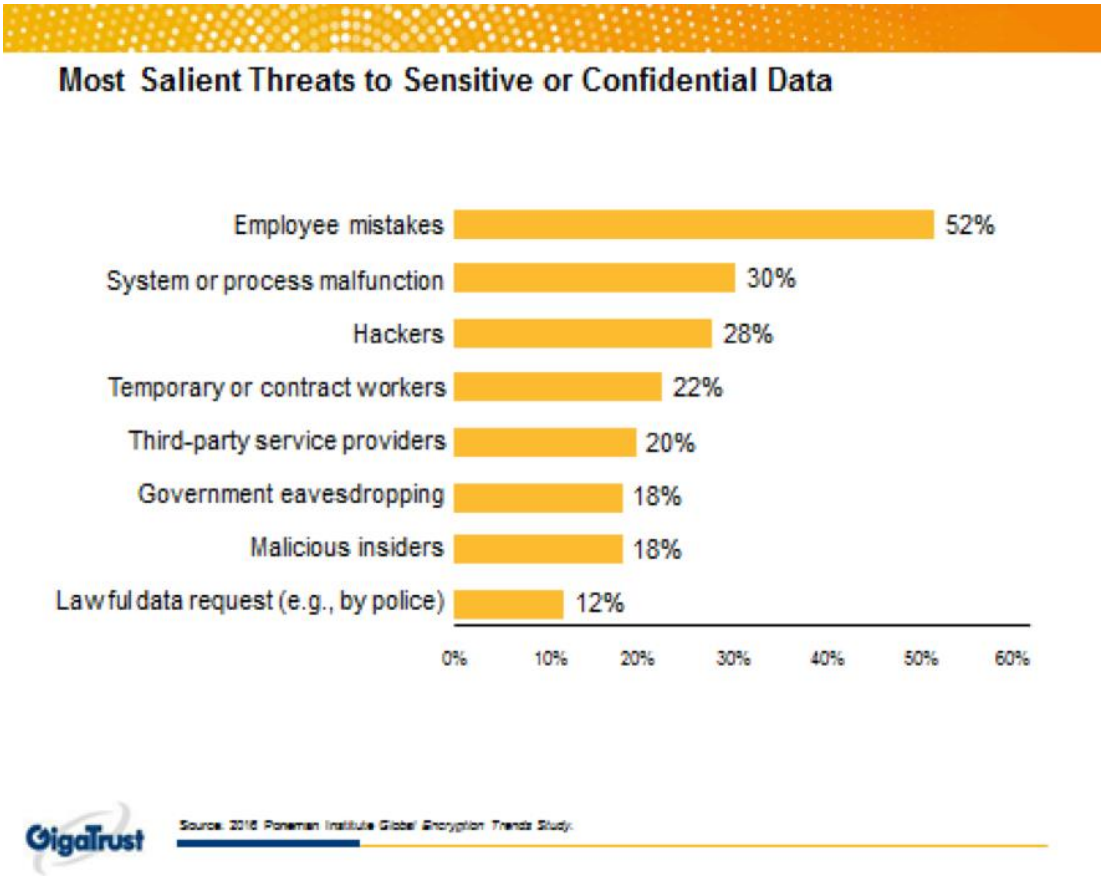
We build a cyber security culture. A what? Think of it like a moat surrounding a castle, protecting the king from invaders. Only in this case, the king is PII, proprietary data, intellectual capital, medical information, legal documents, anything that should only be seen by the people and organizations selected and sanctioned by you. Not to mention that content protection meets compliance regulations. The moat—the cyber security culture—is designed to mitigate the risk of data leakage by establishing endpoint protection with guidelines communicated to employees for operating safely in a digital world, ensuring guardrails are in place.

**Protect the castle—protect the king**

We all know content is king—whether it's personal or business related. And we know the importance of protecting it. Building a cyber security culture starts with understanding the importance of content protection—at rest, in use and in transit. Each employee must have a stake in protecting content through an allegiance to the organization's values and goals, supporting their vision and mission. Incorporating a cyber security program within corporate governance policy is an effective way of inculcating cyber security mindfulness in your organization. Cyber security awareness is most successful communicated from the top down—and practiced.

Over 30 major data breaches have occurred so far in 2017. Hard to believe, but true. The list includes retail, financial services, technology, health care, hospitality, educational institutions, professional services, and government agencies—all hit. Is there something that can be done to prevent this from happening again?

**Step 1** is awareness—we've covered that. But unfortunately, it's not that simple. Employee mistakes are the number one reason for data breaches. That's why an awareness program is mission-critical. Continuing education about content protection must be a major component of the program.




**Step 2** is equally as important. It's the organization's commitment to implement a solution that delivers persistent content protection and endpoint security inside and outside the firewall.

The GigaTrust™ flagship service, GigaCloud™, meets the criteria of Step 2. It delivers persistently protected emails and documents for collaboration anytime, anywhere, to anyone on virtually any device and serves as the foundation of a well-rounded cyber security culture. GigaCloud is the first and only secure email and document protection, consumption, and collaboration service that is an easy-to-use, easy-to-deploy private or multi-tenant cloud service powered by the Microsoft – Active Directory Rights Management Services (AD RMS) security ecosystem.

Long live persistently protected content—supported by a cyber security culture.